IN THE SPECIFICATION:

Please amend paragraph [0001] beginning on page 1, at line 8 as set forth below:

This patent application is related to co-pending U.S. Patent Application Serial No. 10/003,501; ~~Attorney Docket No. 10014010-1~~, entitled "METHOD AND COMPUTER READABLE MEDIUM FOR SUPPRESSING EXECUTION OF SIGNATURE FILE DIRECTIVES DURING A NETWORK EXPLOIT"; U.S. Patent Application Serial No. 10/001,431; ~~Attorney Docket No. 10016933-1~~, entitled "SYSTEM AND METHOD OF DEFINING THE SECURITY CONDITION OF A COMPUTER SYSTEM"; U.S. Patent Application Serial No. 10/001,410; ~~Attorney Docket No. 10017028-1~~, entitled "SYSTEM AND METHOD OF DEFINING THE SECURITY VULNERABILITIES OF A COMPUTER SYSTEM"; U.S. Patent Application Serial No. 10/002,695; ~~Attorney Docket No. 10017029-1~~, entitled "SYSTEM AND METHOD OF DEFINING UNAUTHORIZED INTRUSIONS ON A COMPUTER SYSTEM"; U.S. Patent Application Serial No. 10/002,423; ~~Attorney Docket No. 10017055-1~~, entitled "NETWORK INTRUSION DETECTION SYSTEM AND METHOD"; U.S. Patent Application Serial No. 10/001,445; ~~Attorney Docket No. 10016861-1~~, entitled "NODE, METHOD AND COMPUTER READABLE MEDIUM FOR INSERTING AN INTRUSION PREVENTION SYSTEM INTO A NETWORK STACK"; U.S. Patent Application Serial No. 10/003,815; ~~Attorney Docket No. 10016862-1~~, entitled "METHOD, COMPUTER-READABLE MEDIUM, AND NODE FOR DETECTING EXPLOITS BASED ON AN INBOUND SIGNATURE OF THE EXPLOIT AND AN OUTBOUND SIGNATURE IN RESPONSE THERETO"; U.S. Patent Application Serial No. 10/001,446; ~~Attorney Docket No. 10016591-1~~, entitled "NETWORK, METHOD AND COMPUTER READABLE MEDIUM FOR DISTRIBUTED SECURITY UPDATES TO SELECT NODES ON A NETWORK"; U.S. Patent Application Serial No. 10/003,747; ~~Attorney Docket No. 10014006-1~~, entitled "METHOD, COMPUTER READABLE MEDIUM, AND NODE FOR A THREE-LAYERED INTRUSION PREVENTION SYSTEM FOR DETECTING NETWORK EXPLOITS"; U.S. Patent Application Serial No. 10/002,072; ~~Attorney Docket No. 10016864-1~~, entitled "SYSTEM AND METHOD OF AN OS-INTEGRATED INTRUSION DETECTION AND ANTI-VIRUS SYSTEM"; U.S. Patent Application Serial No. 10/002,697; ~~Attorney Docket No. 10002019-1~~, entitled "METHOD,

NODE AND COMPUTER READABLE MEDIUM FOR IDENTIFYING DATA IN A NETWORK EXPLOIT"; U.S. Patent Application Serial No. 10/003,820; ~~Attorney Docket No. 10017334-1~~, entitled "NODE, METHOD AND COMPUTER READABLE MEDIUM FOR OPTIMIZING PERFORMANCE OF SIGNATURE RULE MATCHING IN A NETWORK"; U.S. Patent Application Serial No. 10/003,819; ~~Attorney Docket No. 10017333-1~~, entitled "METHOD, NODE AND COMPUTER READABLE MEDIUM FOR PERFORMING MULTIPLE SIGNATURE MATCHING IN AN INTRUSION PREVENTION SYSTEM"; U.S. Patent Application Serial No. 10/002,694; ~~Attorney Docket No. 10017330-1~~, entitled "USER INTERFACE FOR PRESENTING DATA FOR AN INTRUSION PROTECTION SYSTEM"; U.S. Patent Application Serial No. 10/001,728; ~~Attorney Docket No. 10017270-1~~, entitled "NODE AND MOBILE DEVICE FOR A MOBILE TELECOMMUNICATIONS NETWORK PROVIDING INTRUSION DETECTION"; U.S. Patent Application Serial No. 10/003,510; ~~Attorney Docket No. 10017331-1~~, entitled "METHOD AND COMPUTER-READABLE MEDIUM FOR INTEGRATING A DECODE ENGINE WITH AN INTRUSION DETECTION SYSTEM"; and U.S. Patent Application Serial No. 10/001,350; ~~Attorney Docket No. 10017303-1~~, entitled "SYSTEM AND METHOD OF GRAPHICALLY CORRELATING DATA FOR AN INTRUSION PROTECTION SYSTEM".

Please amend the paragraph beginning on page 7, line 11, and extending through page 8, line 8, as set for below:

A protocol decode engine 24 is often utilized in conjunction with a network capture system and facilitates efficient analysis of the information obtained by the network capture system. Decode engine 24 is typically a software application that reads raw network data, such as binary streams captured off an Ethernet, and converts the captured data into a format suitable for viewing and analysis by a network manager or security personnel. Decode engine 24 is integrated within intrusion protection system 14 to simplify interpretation of intrusion-related network traffic. An exemplary three layered intrusion protection system 14 comprises an application service provider, a transport service provider and a network filter service

provider is described in co-pending application entitled Method and Computer Readable Medium for a Three-Layered Intrusion Prevention System for Detecting Network Exploits ~~[10014006-1]~~, ~~Ser. No. _____~~ U.S. Patent Application Serial No. 10/003,747, and a protocol decode engine integrated with an intrusion protection system is described in co-pending patent application entitled Method and Computer-Readable Medium for Integrating a Decode Engine with an Intrusion Detection System ~~[10017331-1]~~, ~~Ser. No. _____~~ U.S. Patent Application Serial No. 10/003,510. As network driver 20 or another component of the intrusion protection system recognizes an attack, packet data associated with that intrusion event, or event data, are logged or stored in event database 22. Intrusion events are defined by a "signature" or a data pattern that may be used to identify a known attack. For example, a distributed attack commonly known as the "ping of death" has the telltale signature of particular series of bits in the ICMP (Internet Control Message Protocol) header and IP (Internet Protocol) header. This may be expressed as:

(icmp) & (65535 < ((ip[2:2] - ((ip[0:1] 0x0f)*4)) + ((ip[6:2]_0x1fff) * 8))))

Event logging may comprise writing a copy of the network frame or packet identified in the intrusion event, reporting an indication of the signature file(s), such as a signature file identification index, determined to have a correspondence with the identified frame or packet, date and time of the event, indexing the event with an event number, as well as logging other intrusion event information. The signature definitions of known attacks are preferably stored in a database 26.